MÉTHODES DE PREUVES

IFT1065 – AUT. 2007

1. INTRODUCTION

Un système mathématique (ou axiomatique) comprend un certain nombre d'**axiomes** (d'énoncés admis comme vrais) et de **définitions** (qui permettent de créer de nouveaux concepts). Les conséquences des axiomes, obtenues par une argumentation logique appelée **preuve**, sont appelées **théorèmes**, **lemmes**, **corollaires**[1]

Théorème: Résultat principal

Lemme: Résultat intermédiaire, qui sert à prouver un théorème

Corollaire: Résultat qui découle directement d'un théorème

Exemple 1. *L'arithmétique des entiers naturels est un système mathématique. Parmi les **axiomes**, on a que pour tout entier n, $n \times 1 = n$, que pour tout m et n, $m \times n = n \times m$ etc. Parmi les **définitions**, on a qu'un entier naturel p est dit premier s'il n'a d'autre facteurs que 1 et lui-même ; donc 5 est premier mais pas* 6 *(* $= 2 \times 3$*). Parmi les **théorèmes**, on a que tout entier naturel peut s'exprimer comme un produit de nombres premiers. Un autre **théorème** dit qu'il y a une infinité de nombres premiers. Un **corollaire** est qu'il n'y a pas de plus grand nombre premier.*

2. PREUVES DÉDUCTIVES

2.1. **Preuves directes.** Pour déduire que pour tout $x_1, \ldots, x_n$, $q(x_1, \ldots, x_n)$ est vrai sachant que pour tout $x_1, \ldots, x_n$, $p(x_1, \ldots, x_n)$ et vrai, on procède comme suit :

- On suppose que $p(x_1, \ldots, x_n)$ est vraie pour des valeurs quelconques de $x_1, \ldots, x_n$
- On déduire $q(x_1, \ldots, x_n)$

Exemple 2.

(1) *Donner une définition rigoureuse d'un entier **pair** et d'un entier **impair**.*

(2) *Montrer que pour tout entier m et tout entier n, si m est pair et n impair, alors $m + n$ est impair.*

[1] Il y a aussi des **propositions** qui sont des théorèmes de moindre importance.

2.2. **Preuves par contradiction (ou preuves par l'absurde).** On les appelle aussi preuve indirectes. Elles sont basées sur le fait que $p \Rightarrow q \equiv (p \wedge \neg q) \Rightarrow (r \wedge \neg r)$. Rappelons que $r \wedge \neg r$ est une contradiction.

Méthode : Pour démontrer que

$$p(x_1, \ldots, x_n) \Rightarrow q(x_1, \ldots, x_n)$$

par preuve par contradiction, on procède comme suit :

- On suppose $p(x_1, \ldots, x_n)$
- On suppose $\neg q(x_1, \ldots, x_n)$ (i.e. que $q(x_1, \ldots, x_n)$ est faux)
- On en déduit une contradiction (ou une absurdité).

Exemple 3.

(1) *Si $x + y \geq 2$ avec, x et y réels, alors $x \geq 1$ ou $y \geq 1$.*

(2) *Si m est entier et m^2 est impair, alors m est impair.*

2.3. **Preuve par contrapositive.** On utilise l'équivalence $p \Rightarrow q \equiv \neg q \Rightarrow \neg p$. Pour prouver que p implique q, on suppose $\neg q$ et on déduit $\neg p$.

2.4. **Preuve par cas.** Basée sur $(p_1 \vee p_2 \vee \ldots \vee p_n) \Rightarrow q \equiv (p_1 \Rightarrow q) \wedge (p_2 \Rightarrow q) \wedge \ldots \wedge (p_n \Rightarrow q)$.

Pour démontrer que $(p_1 \vee p_2 \vee \ldots \vee p_n) \Rightarrow q$, par preuve par cas on démontre que
- $p_1 \Rightarrow q$
- $p_2 \Rightarrow q$
- $\ldots$
- $p_n \Rightarrow q$

Exemple 4.

(1) *Montrer que pour tout x réel, $x \leq |x|$*

(2) *Montrer que pour tout n entier, $n(n+1)$ est pair.*

2.5. **Condition nécessaire et suffisante.** Certains théorèmes s'expriment ainsi : "Pour que p soit vrai, il faut et il suffit que q soit vrai". Ceci signifie que $p \Leftrightarrow q$ et la preuve consiste à prouver que p implique q et que q implique p.

Exemple 5. *Pour tout entier n, pour que n soit pair il faut et il suffit que $n-1$ soit impair.*

2.6. **Preuve existentielle.** Pour prouver que $\exists x \mathrm{P}(x)$ la preuve existentielle **exhibe une valeur** de x pour laquelle $\mathrm{P}(x)$ est vraie.

Exemple 6. *Soient $a < b$, $a, b \in \mathbf{R}$. Montrer $\exists x \in \mathbf{R} \mid ((a < x) \wedge (x < b))$*

2.7. **Preuve par contre exemple.** Pour prouver que $\forall x \mathrm{P}(x)$ est faux on exhibe un x pour lequel $\mathrm{P}(x)$ est faux.

Exemple 7. *La proposition "$\forall n \in \mathbf{N}, 2^n + 1$ est premier" est fausse.*

3. Preuve par induction mathématique

Soit $\mathrm{P}(n)$ un prédicat dont le domaine contient les entiers supérieurs ou égaux à n_0. Si l'on peut prouver que

(1) $\mathrm{P}(n_0)$ est vrai

(2) Pour n arbitraire, $\quad (n \geq n_0) \wedge \mathrm{P}(n) \Rightarrow \mathrm{P}(n+1)$

alors le principe d'induction mathématique nous permet de déduire de (1) et (2) que

$$\mathrm{P}(n) \text{ est vrai pour tout } n \geq n_0$$

(1) est dit le **cas de base** et **(2)** est appelée **étape inductive** ou **pas d'induction**.

Exemple 8. *Pour n entier, $n \geq 1$, posons $\mathrm{S}_n = 1 + 2 + \ldots + n$. Donc $\mathrm{S}_1 = 1$, $\mathrm{S}_2 = 1 + 2 = 3$, $\mathrm{S}_3 = 1 + 2 + 3 = 6$, Démontrer que pour tout $n \geq 1$,*

$$\mathrm{S}_n = \frac{n(n+1)}{2}$$

par induction mathématique

Définition 1. *On définit $n!$, la **factorielle** de n comme suit*

$$n! = \begin{cases} 1 & si\ n = 0 \\ n \times (n-1)! & si\ n \geq 1 \end{cases}$$

Cette définition se traduit informellement par $n! = n \times (n-1) \times \ldots \times 1$ pour $n \geq 1$ et $0! = 1$.

Exemple 9. *Démontrer par induction mathématique que pour tout entier $n \geq 1$, $n! \geq 2^{n-1}$.*

Exemple 10. *Démonter que pour $r \neq 1$ et $n \geq 0$*

$$a + ar^1 + \ldots + ar^n = \frac{a(r^{n+1} - 1)}{r - 1} \tag{3.0.1}$$

pour tout $n \geq 0$.

Quelle est la valeur de

$$1 + \frac{1}{2} + \frac{1}{4} + \ldots + \frac{1}{2^n} ?$$

L'induction mathématique permet de prouver qu'une formule ou une conjecture est vraie, elle ne permet pas de trouver la formule. Dans les publications scientifiques, elle sert à convaincre les autres chercheurs de ce dont on est soi-même convaincu.

Exemple 11. *Montrer que $5^n - 1$ est divisible par 4 pour tout $n \geq 1$.*

Exemple 12. *Un farfelu veut nous prouver que $n \geq 1$ boules de billard sont toujours de la même couleur. Pour ce faire, il utilise le principe d'induction et affirme :*

(1) *Si $n = 1$ il n'y a qu'une seule boule, elles sont toutes de la même couleur.*

(2) *Si $n \geq 1$ boules de billard sont toujours de la même couleur on peut en déduire que $n+1$ boules sont alors toutes de la même couleur. En effet, soient $n+1$ boules :*
   - *si on enlève une boule des $n+1$; il en reste clairement n et elles sont par hypothèse toutes de la même couleur.*
   - *Reste à tester la boule que l'on a en mains. On la remet en place et l'on en prend une deuxième. Les n boules qui restent sont encore de la même couleur. La première boule avait donc la même couleur que les autres et les $n+1$ boules sont donc de la même couleur.*

(3) *On en déduit par le principe d'induction que $n \geq 1$ boules de billard sont nécessairement toujours de la même couleur.*

Où est l'attrape ?

4. Induction généralisée et bon ordre

4.1. **Induction généralisée.** Soit $P(n)$ un prédicat défini (au moins) sur les entiers supérieurs ou égaux à n_0.

Si :

(1) $P(n_0)$ est vrai

(2) Pour tout $n > n_0$, si $P(k)$ vrai pour tous les k t.q $n_0 \leq k < n$, alors $P(n)$ l'est aussi

Alors : $P(n)$ est vrai pour tout $n \geq n_0$.

Exemple 13. *Montrer que tout montant de 4 cents ou plus peut être obtenu avec uniquement des timbres de 2 cents et des timbres de 5 cents.*

Dans l'exemple qui suit $\lfloor n/2 \rfloor$ dénote le quotient entier de n par 2 ; $\lfloor 4/2 \rfloor = 2$, $\lfloor 5/2 \rfloor = 2$. Pour $n > 1$ on a $1 \leq \lfloor n/2 \rfloor < n$.

Exemple 14. *Soit c_n définie par*

(1) $c_1 = 0$

(2) $c_n = c_{\lfloor n/2 \rfloor} + n$ *si* $n > 1$

Montrez que pour $n \geq 1$, $c_n < 4n$

4.2. **Principe du bon ordre.** Tout ensemble non vide d'entiers positifs a un plus petit élément.